(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 661 843 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
10.11.1999 Bulletin 1999/45

(43) Date of publication A2:
05.07.1995 Bulletin 1995/27

(21) Application number: **94119371.6**

(22) Date of filing: **08.12.1994**

(51) Int. Cl.[6]: **H04L 9/22**

(84) Designated Contracting States:
BE DE FR GB IT NL SE

(30) Priority: **31.12.1993 ES 9302742**

(71) Applicant:
ALCATEL STANDARD ELECTRICA, S.A.
28045 Madrid (ES)

(72) Inventor:
Alvarez Alvarez, Manuel José
E-28820 Coslada (Madrid) (ES)

(74) Representative:
Feray, Valérie et al
Alcatel Espana S.A.
Patent Department
Ramirez de Prado 5
28045 Madrid (ES)

(54) Device for implentation of DECT encryption algorithm with reduced current consumption

(57) The invention has application to the implementation of the DECT standard data ciphering algorithm which requires a lengthy procedure of key loading and logic operations during the stages of pre-ciphering and ciphering and requiring clocks operating at different frequencies.

This device performs parallel mode loading of the shift registers, with a ciphering keyword. It also calculates, in a first cycle, during the pre-ciphering, the values of the bits of each shift register that determine the value of the next shift in order to, in a second cycle, effect parallel mode shifting in these registers with a value equal to the sum of the two previous shift values.

During the ciphering process, the shifting is done in the registers, in parallel mode and in a single data clock cycle, with a value equivalent to the serial value obtained by the algorithm.

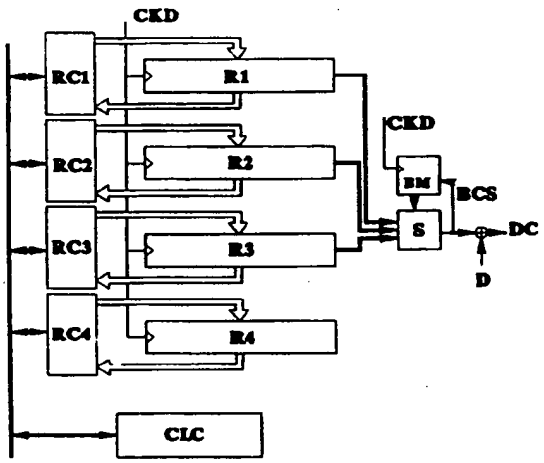

FIG. 5

EP 0 661 843 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 11 9371

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	US 4 211 891 A (GLITZ EKKEHARD) 8 July 1980 (1980-07-08) * column 3, line 15 - column 4, line 2 * * column 4, line 32 - line 56 * ---	1,4,5	H04L9/22
A	FR 2 619 976 A (MOULY MICHEL) 3 March 1989 (1989-03-03) * page 2, line 14 - line 17 * * page 2, line 33 - page 4, line 13 * * page 5, line 9 - page 6, line 17 * ---	1	
A	HUGHES M T G: "Transition-matrix construction for pseudorandom binary-sequence generators" ELECTRONICS LETTERS, SEPT. 1968, UK, vol. 4, no. 19, pages 417-419, XP002115367 ISSN: 0013-5194 * the whole document * -----	2	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	15 September 1999	HOLPER, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 94 11 9371

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-09-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4211891 A	08-07-1980	DE 2706421 B	29-06-1978
		AT 376344 B	12-11-1984
		AT 87678 A	15-03-1984
		CH 639229 A	31-10-1983
		FR 2381423 A	15-09-1978
		GB 1598415 A	23-09-1981
		NL 7801619 A	18-08-1978
FR 2619976 A	03-03-1989	NONE	